IN THE CLAIMS:

1. (Currently Amended) A logic circuit for encrypting and decrypting data including shifting in a MixColumn transform by multiplication of an (m x n) matrix of data by a (1 x n) or by a (m x 1) matrix, where m is a number of rows and n is a number of columns, and wherein each successive row m of n elements is a predetermined row permutation of a preceding row, the circuit comprising:

n multiplication circuits for performing a multiplication function on a value of data, each n multiplication circuit having ~~an~~a data input for receiving input data and an output ~~which returns the~~for outputting a changed value of the data received by said input, the output value of the data comprising the input data that has been multiplied by a predetermined multiplicand;

n logic circuits, each logic circuit comprising at least a first input and a second input for executing a predetermined logical combination of athe first input and athe second input to provide a logical output, the first input being coupled to the output of a corresponding one of the n multiplication circuits;

n registers coupled to said n logic circuits for receiving and storing said logical output from a respective logic circuit;

feedback logic for routing ~~the~~ stored contents of each register to a selected one of the second inputs of said n logic circuits in accordance with a feedback plan that corresponds to ~~the~~a predetermined row permutation; and

control means for successively providing ~~as~~a data input to each of the n multiplication circuits for each element in the (1 x n) or (m x 1) matrix; and

wherein said n registers in accordance with said feedback logic having a data-shifted output of the data input by the control means, the data-shifted output in each of the n registers having a state "s" for remaining encryption or decryption operations.

2. (Original) The logic circuit of claim 1 in which the feedback logic provides a feedback plan corresponding to said predetermined row permutation that is a row shift.

3. (Original) The logic circuit of claim 2 in which the row shift is a single element right shift.

4. (Original) The logic circuit of claim 1 in which the n logic circuits are each adapted to execute an XOR-combination of said first input and said second input.

5. (Original) The logic circuit of claim 1 in which each of the predetermined multiplicands corresponds to one of the elements in the AES Rijndael MixColumns transform function.

6. (Original) The logic circuit of claim 5 in which the number m=4, the number n=4, the multiplicand for the first multiplication circuit=02, the multiplicand for the second multiplication circuit=03, the multiplicand for the third multiplication circuit=01, and the multiplicand for the fourth multiplication circuit=01.

7. (Original) The logic circuit of claim 5 in which the number m=4, the number

n=4, the multiplicand for the first multiplication circuit=0E, the multiplicand for the second multiplication circuit=0B, the multiplicand for the third multiplication circuit=0D, and the multiplicand for the fourth multiplication circuit=09.

8. (Currently Amended) The logic circuit of ~~claim 6in~~ claim 6, in which the four multiplicands are ~~switchable~~switched between the values in claim 6.

9. (Original) The logic circuit of claim 1 in which the control means is adapted to successively provide as input to each of the n multiplication circuits each successive element in the (1.times.n) or (m.times.1) matrix over each of n or m cycles of operation respectively.

10. The logic circuit of claim 1 in which each of the n multiplication circuits, each of the n logic circuits, and each of the n registers are at least eight bits wide.

11. (Original) The logic circuit of claim 1 in which the control means further includes means for providing as output from said logic circuit the contents of the n registers after each nth cycle.

12. (Original) The logic circuit of claim 1 in which the control means further includes means for resetting each of the registers prior to the first calculation cycle.

13. (Original) The logic circuit of claim 1 in which each successive row m of n

elements is a predetermined row permutation of the immediately preceding row.

14. (Currently Amended) An AES MixColumns transform circuit incorporating the logic circuit of ~~any one of claims 1 to 13~~claim 1.

15. (Currently Amended) An AES encryption and/or decryption engine incorporating the logic circuit ~~of claim 1~~ for performing the MixColumns transform, said logic circuit for multiplication of an matrix by a or by a matrix, where m is a number of rows and n is a number of columns, and wherein each successive row m of n elements is a predetermined row permutation of a preceding row, the circuit comprising:

n multiplication circuits each having an input and an output which returns the value of said input multiplied by a predetermined multiplicand;

n logic circuits, each for executing a predetermined logical combination of a first input and a second input to provide a logical output, the first input being coupled to the output of a corresponding one of the n multiplication circuits; n registers for receiving said logical output;

feedback logic for routing the contents of each register to a selected one of the second inputs in accordance with a feedback plan that corresponds to the predetermined row permutation; and

control means for successively providing as input to each of the n multiplication circuits each element in the or matrix.

16. (Canceled)

17. (New) A smartcard comprising the logic circuit according to claim 1.

18. (New) A method for encrypting and decrypting data including shifting in a MixColumn transform by multiplication of an (m x n) matrix of data by a (1 x n) or by a (m x 1) matrix, where m is a number of rows and n is a number of columns, and wherein each successive row m of n elements is a predetermined row permutation of a preceding row, comprising the steps of:

successively providing an input to each of n multiplication circuits for each element in the (1 x n) or (m x 1) matrix by a control means;

performing a multiplication function by "n" multiplication circuits on a value of data, each n multiplication circuit having a data input for receiving data and an output for outputting a changed value of the data received by said input, the changed value of the data comprising input data that has been multiplied by a predetermined multiplicand;

executing a predetermined logical combination by n logic circuits to provide a logical output, each logic circuit comprising at least a first input and a second input, the first input being coupled to an output of a corresponding one of the n multiplication circuits;

receiving and storing said logical output from a respective logic circuit of n logic circuits by a register from a plurality of n registers, n registers being coupled to said n logic circuits;

routing the contents of each register to a selected one of the second inputs of said n logic circuits by feedback logic in accordance with a feedback plan that corresponds to a predetermined row permutation; and

storing a data-shifted output of the data input by the control means, the data-shifted output in each of the n registers received by the n registers in accordance with the feedback logic, and the data-shifted output having a state "s" for use in remaining encryption or decryption operations.